SCDC POLICY

NUMBER: ADM-15.05

TITLE: SECURITY AND USEOFINFORMATION TECHNOLOGY

ISSUE DATE: August 3, 2016

RESPONSIBLE AUTHORITY: DIVISION OF RESOURCE AND INFORMATION MANAGEMENT

OPERATIONS MANUAL: ADMINISTRATION

SUPERSEDES: ADM-15.05 (January 17, 2014), (June 1, 2000), (June 15, 1998)

RELEVANT SCDC FORMS/SUPPLIES: 13-50,Appendix A,Appendix B(Appendix B is SCDC Form 13-53),Appendix C(Appendix C is SCDC Form 13-54)

ACA/CAC STANDARDS: 4-ACRS-7D-05, 4-ACRS-7D-08, 4-4100, 4-4101

STATE/FEDERAL STATUTES: Copyright Act (United States Code of Laws, Title 17);South Carolina Public Records Act (Code of Laws of South Carolina, 1976, Sections 30-1-10 through 30-1-140, as amended); South Carolina Freedom of Information Act (Code of Laws, 1976, Sections 30-4-10 through 30-4-165, as amended); Breach of Security of State Agency Data (Code of Laws of South Carolina, 1976, Section 1-11-490, as amended)

DISCUSSION: Access to computer systems and networks owned or operated by SCDC and the State of South Carolina imposes certain responsibilities and obligations on authorized users. Various state and federal statutes, as well as state and Agency policies/procedures, govern the acceptable use of computer software and related information technology (IT) equipment by any authorized user. It is incumbent upon all authorized users to become familiar with these regulations, statutes, and directives and to abide by the same at all times. Any user who violates any copyright declarations or any provisions of the federal Copyright Act (Title 17, U.S. Code) or any other state or federally imposed regulations will be considered as acting outside the scope and course of his/her employment or other authority, and SCDC will be relieved of any legal responsibility that may result therefrom. Users will, therefore, be held personally liable for any monetary or other penalties that may result due to such violations, whether done willfully or unknowingly, or for sale, for free distribution, or for the violators own use. Users may also be held in violation of any state or Agency directive and/or policies and may be subject to related corrective action.

PURPOSE: To establish general guidelines for the security and use of the Internet, electronic mail, and information technology equipment and the information held therein.

POLICY STATEMENT: To promote the safety, security, and best interests of the State, the Agency, its employees, and the public, the South Carolina Department of Corrections will develop and implement procedures regulating the security of all information technology equipment/systems and the information contained within the same. Additionally, SCDC will develop and implement procedures regulating the security and use of the Internet and electronic mail system. All policies will be strictly enforced and will comply with the requirements of related federal and/or state statutes, regulations, codes, and acts. Only computer software and related information technology equipment approved by SCDC will be authorized for use within the Agency by any employee or inmate. (4-ACRS-7D-05, 4-4100)

TABLE OF CONTENTS

1. INTRODUCTION

2. ACCEPTABLE USE

3. CONFIDENTIALITY OF DATA

4. ACCESS REQUESTS

5. ACCESS TERMINATIONS

6. REPORTING PROBLEMS/REQUESTING TECHNICAL SUPPORT

7. TRAINING

8. DATA LOSS RESPONSE PLAN

9. DEFINITIONS

1. INTRODUCTION:

1.1 The SCDC Division of Resource and Information Management (RIM) will develop specific guidelines regarding acceptable use of IT resources, to include personal computers, printers, fax and copy machines, mainframe systems, information reports and documents, electronic mail systems (e-mail), videoconferencing, and the Internet.

1.2 The Division Director of RIM (or an approved designee) will be responsible for approving all computer software and information technology equipment before it is purchased, leased, or used by SCDC. This includes any software purchased by an employee for use on any SCDC owned or operated information technology equipment.

1.3 Personally owned hardware and software that an employee desires to use while on SCDC property and/or to connect to any SCDC information technology equipment must be approved in writing by the Division Director of RIM and the employee's responsible Warden, Division Director, or other higher authority, before the hardware or software is allowed on SCDC property. Please refer to Section 2 of SCDC Policy ADM-15.03, "Information Technology Requests," for specific procedures regarding the use of personally owned hardware and software. SCDC will not be liable for any personally owned information technology equipment that is damaged, stolen, misused, or destroyed while on SCDC property. No employee will be authorized to bring any personally owned hardware or software to SCDC for use by any inmate.

1.4 The Division of RIM and the Division of IT Security will establish strict provisions for inmate use of computers and other related information technology (IT) equipment.

1.5 The Division of RIM and the Division of IT Security will implement procedures and system software to limit access to information systems to authorized users and will monitor and audit system usage with the goal of providing reliable, accurate, and secure information and operational systems while meeting all legal and confidentiality requirements. Users of these services are advised of this monitoring and agree to this practice.

1.6 Agency managers and supervisors are responsible for monitoring employees and inmates for proper use of information technology resources.

1.7 SCDC employees are authorized to use IT, including personal computers, online systems, information reports, e-mail, the Internet, copy machines, and fax machines for the sole purpose of efficiently and effectively carrying out their assigned job duties. At no time may an employee's use of IT interfere with or detract from the mission of the Agency. Employees violating laws related to legal use of IT will be subject to prosecution, and SCDC will not be liable for damages caused by illegal use of IT resources.

1.8 Any person who violates any copyright declarations or any provisions of the Federal Copyright Act (Title 17, U.S. Code) will be considered as acting outside the scope and course of his/her employment or other authority, and SCDC will be relieved of any legal responsibility that may result therefrom. (See Appendix A for general information pertaining to the U.S. Copyright Act.) These persons will, therefore, be held personally liable for any monetary or other penalties that may result due to such violations, whether done willfully or unknowingly, for sale, for free distribution, or for the violator's own use.

1.9 Under the Code of Laws of South Carolina, e-mail messages created/sent or received using the Agency's e-mail system fall under the category of "Agency property" and are considered "public record." Thus, by law, e-mail is not private. Likewise, no employee should have any expectation of privacy with regard to his/her use of any of the Agency's computer systems or networks, nor to the Internet when accessed through Agency resources.

1.10 Per SCDC Policy GA-06.05, "IT Security," Section 2.7.1.2, all users of SCDC systems must sign a confidentiality/acceptable use statement before access is granted and comply with guidelines regarding legal, ethical, responsible, and acceptable use of IT, defined as follows:

1.10.1 Legal Use of IT: Users must comply with all federal, state, and other applicable laws to include, but not limited to, the laws of privacy, copyright, licensing, libel, obscenity and child pornography, computer fraud, and the Electronic Communications Privacy Act.

1.10.2 Ethical and Acceptable Use: Users must use IT resources within the limit of their authorization and abstain from personal use of resources or disclosure of information for personal purposes. Users have the responsibility to report policy violations, including incidents where information or equipment is inappropriately accessed or used.

1.10.3 Responsible Use: SCDC employees are expected to conserve and protect IT resources, respect competing user need and priorities, and accept IT usage responsibilities to include IT security and reporting of violations. Employees must understand that unwarranted use of the Internet and e-mail can degrade overall system performance and increase the Agency's cost of operating computer and telecommunications systems. Agency managers are expected to authorize and monitor use of IT by employees under their supervision. All employees are responsible for protecting IT equipment and information from damage, theft, and misuse.

1.11Inmates will not have general access to computers or other information technology equipment, except as authorized by the Divisions of RIM and IT Security. The Division of RIM will institute procedures for requesting, authorizing, and monitoring inmate access to IT resources. Under no circumstances will inmates be allowed to use computers with direct access to the Agency's network or the Internet.

2. ACCEPTABLE USE:
2.1 Legal Use of IT Resources:

2.1.1 Per SCDC Policy GA-06.05, "IT Security," Section 2.7.1, all users must sign an acknowledgment agreeing to abide by SCDC policies and procedures in their use of IT resources and are subject to prosecution for violation of State and Federal laws relating to any illegal use of IT. Examples of specific unlawful use include:

- Privacy and Confidentiality of Information: certain personally identifiable information, in particular health and medical history data, is protected by Federal statute.
- Computer Security: It is illegal for employees to break in to, or attempt to break in to any computer system to which they are not authorized. Employees must not use, or attempt to use, another's logon ID and/or password.

•Computer Crime: Use of computers, fax machines, or other IT resources to obtain confidential information in order to commit fraud is expressly prohibited by law.

•Copyright and Licensing Laws: Employees must not copy or propagate software that is licensed to SCDC, must not install software that is not owned by SCDC on Agency equipment, and must not reproduce copyrighted information or publications.

•Use of the Internet, e-mail, or other IT resources for child exploitation, pornography, harassment, or libel is illegal and is subject to prosecution under the law.

•Unauthorized use of SCDC IT resources for profit or personal gain constitutes fraud and/or theft and is subject to restitution and/or legal prosecution.

2.1.2 The Division of RIM and the Division of IT Securitywill randomly audit personal computers to detect and forestall unauthorized use of IT resources. Employees who violate State or Federal law while using SCDC IT resources are subject to disciplinary action under SCDC Policy ADM-11.04, "Employee Corrective Action," and are subject to prosecution. SCDC will not be liable for such violations, and may require restitution from employees.

2.2 Ethical and Acceptable Use of IT Resources:

2.2.1 Employees will be prohibited from taking any SCDC information technology equipment, data, or files from the Agency upon their retirement, termination, suspension, resignation, or transfer to another state Agency without the express written approval of the Agency Director or designee.

2.2.2 Unless authorized by the Division Director of RIM, employees are not allowed to install or load software on SCDC equipment, are not allowed to bring personally owned equipment or software to SCDC, and are prohibited from accepting donated or borrowed equipment and software unless authorized in accordance with SCDC Policy ADM-15.03, "Information Technology Requests."

2.2.3 Unless explicitly allowed by SCDC Policy or authorized by the Division Director of RIM, employees are prohibited from taking IT equipment off SCDC premises. The Division of RIM provides a limited amount of equipment, including laptop computers, projectors, cell phones, and pagers that may be "signed out" for official, off-site use. Employees will be financially responsible for damage to, or loss of "sign out" equipment.

2.2.4 Users will assume responsibility for any charges associated with billable services unless appropriate authorization has been obtained from the Division Director of RIM.

2.2.5 The Division of RIM allows employees to access SCDC systems and e-mail off-site using their personal, public Internet Service Providers (ISP). Unless authorized by the Division Director of RIM, SCDC will not reimburse employees for costs incurred to connect to SCDC systems while off-site and will not purchase or provide telecommuting equipment.

2.2.6 In accordance with SCDC Policy ADM-15.03, "Information Technology Requests," IT equipment must not be moved and no attempt should be made to repair IT equipment without authorization from the Division of RIM.

2.2.7 Employees must log off computer systems when not in use. Employees must not leave IT resources (e.g., computers, copiers, fax machines, printouts, and supplies) unattended in areas where inmates have access.

2.2.8 Employees must not allow inmates to use IT equipment resources without proper authorization as described in the procedures below. Employees supervising inmates with authorization to use IT are responsible for monitoring and auditing inmate use of the equipment/information, and are responsible for reporting any violations to the Division of RIM.

2.2.9 Each user who has been assigned a user ID will be responsible for keeping his/her password secret and for all information entered into the computer under his/her user ID. Any user who reveals his/her password to another user, employee, inmate, or other person: signs-on to any terminal/PC or other related information technology equipment and permits another to request or enter information; or misuses a terminal/PC or other information technology equipment may be subject to corrective action pursuant to SCDC Policy ADM-11.04, "Employee Corrective Action."

2.2.10 Users will be required to change theirpassword every 60 days. Passwords must be eight characters in length and must include at least 1 character, 1 number, and 1 special symbol ( # $ @ ). The password must be a combination of letters and numbers and special symbols that the user has not used previously. Users must not create a password that is easily guessed, must not share their password with anyone, and must not write down their password. Users must immediately change their password if they suspect anyone else may know it, and must promptly report possible security breaches to the RIM Help Desk.

2.2.11 The repeated use of an invalid password by any user will result in the user being revoked from the automated system. Users are responsible for notifying the RIM Help Desk whenever they are revoked. The Help Desk will be responsible for re-setting a revoked user ID and notifying, using a secure method, the user of the temporary password that has been established to allow the user one-time access to the system to create a new password. For security reasons, the Help Desk will ask the user to verify his/her identity by asking questions that only he/she would be able to answer.

2.2.12 Users will maintain the security of all assigned computer equipment, restricted user manuals, and management reports. Employees must not share or disclose private individual information pertaining to employees, victims, witnesses, or inmates. Looking up information outside the purview of an employee's

functional responsibility, or using such information for personal reasons, constitutes unacceptable use of IT.

2.2.13 Users must secure printouts, documents, diskettes, and related materials and must shred documents containing confidential information. Diskettes, CDs, DVDs, USB drives, and any other types of removable media must be shredded or otherwise physically destroyed prior to disposal.

2.2.14 The intentional destruction of data or of any information technology will be prohibited and may result in the employee being disciplined and/or prosecuted pursuant to applicable SCDC directives and/or state and federal statutes.

2.2.15 Users are authorized to use SCDC approved information technology equipment only for official state business to access only files and data that are their own, that are publicly available, or to which they have been given authorized access. Authorized employees may use the Internet and electronic mail system for official job duties only (to access/exchange work-related information, to maintain job knowledge or skills, to research and gather work-related information, to communicate for administrative purposes, etc.). Employees will "unsubscribe" to irrelevant e-mail distributions, will not provide their e-mail address to persons or organizations that are not associated with their job duties, will not use "instant messaging" or enter Internet "chat" rooms, and will not connect to Internet broadcasts that are not pertinent to their job assignment.

2.2.16 Users will not use Agency IT resources including computers, Agency networks, the Internet, and electronic mail system for private, personal, recreational, or any other non-Agency purposes including the conduct of personal commercial/business transactions, advertising/marketing of private products or services, political activities, not-for-profit fund-raising or public relations, or any other unauthorized activities.

2.2.17 Personal use of fax machines, printers, and copiers is prohibited.

2.2.18 Users are not allowed to use "dial up" modems, outside Internet Service Providers, Virtual Private Networks (VPNs), TOR or similar protocols to access any type of web service.

2.2.19 Users are not allowed to use any type of remote desktop software while on SCDC premises or to connect to SCDC systems remotely without prior authorization by the Division of RIM and the Division of IT Security.

2.2.20 Users are not allowed to use any operating system other than the one installed on his/her PC by the Division of RIM without prior authorization by the Division of RIM and the Division of IT Security.

2.2.21The Division of RIM and the Division of IT Security will audit computer access annually, will routinely inspect computers for indication of inappropriate use, will implement security mechanisms to prevent access to unacceptable web sites, and will install software to detect and prevent computer viruses.

2.3 Responsible Use of IT Resources:

2.3.1 Employees must treat equipment with care and seek to prevent damage to equipment. Employees must not eat or drink while using PCs or terminals, must keep all equipment clear of potted plants, leaking roofs, and plumbing, and must protect equipment from intense heat, dust, and strong magnetic fields.
2.3.2 Employees should report problems such as equipment malfunctions to the RIM Help Desk, providing as much information as possible regarding the problem. In particular, employees must promptly notify the Help Desk if they suspect existence of a computer virus or any other type of threat to the security of Agency IT systems.
2.3.3Employees must attempt to use/share existing equipment before requesting procurement of additional equipment. Printers, copiers, and fax machines will normally be shared by as many employees as possible.
2.3.4Employees are responsible for accuracy of data entries. The system will automatically record the date and person making critical entries. RIM will provide Agency managers with analysis of data entries to assist with data audits and reviews of employee performance.
2.3.5 Documents and files should be downloaded from the Internet only when directly relevant to job duties and when the source of the information is known and trusted. To guard against computer viruses, employees will not "open" documents or files that are attached to e-mail unless from a known/trusted source and only when the attachment is directly related to job duties. Forwarding e-mail or attachments that contain jokes, games, or other material that is irrelevant to their job duties is considered unacceptable use of IT.
2.3.6Employees will not store important documents/files on local hard drives or removable media such as diskette, CD/DVD, USB drives, etc. Important documents/files will be stored on network drives where they can be backed up by the Division of RIM and recovered in the event of accidental deletion, hardware failure, virus infection, etc. Employees will not store large documents on the network, in particular, videos, pictures, and sound files, unless there is a legitimate need for the material.
2.3.7 The Divisions of RIMand IT Security will routinely monitor network traffic and computer servers to maintain an acceptable level of system performance and to detect possible viruses, malfunctions, and over burdened systems. Users will not attempt to intercept network traffic for any purpose unless engaged in authorized network administrative duties.
2.3.8 Any user that loses, misplaces, or has SCDC equipment stolen must report the occurrence to Help Desk as soon as he/she becomes aware of the loss.
2.4 Inmate Use of IT Resources:

2.4.1 Inmates are allowed to use designated inmate kiosks as his/her institutional schedule allows, to access approved inmate services such as trust fund balance inquiry, electronic messaging, and canteen ordering. These kiosks are specially secured and exempt from the provisions in the remainder of this section. Employees who observe or suspect any unapproved use of the inmate kiosks must report this immediately to the Warden, Division Director of IT Security,and Division Director of RIM.

2.4.2 Inmates are allowed to use designated computers to access legal resources, if available in their institution. These computers are connected to a dedicated, secure network allowing access to only the approved legal research materials, and are exempt from the provisions in the remainder of this section. Employees who observe or suspect any unapproved use of the inmate law library computers must report this immediately to the Warden, Division Director of IT Security and Division Director of RIM.

2.4.3 Inmates enrolled in specific academic or vocational education programs are allowed to use computers in conjunction with the associated curriculum, if these computers are not connected to any network outside the computer lab/school. Instructors are responsible for ensuring that inmate use of computer equipment is limited to the specific educational program and for immediately reporting any violations relating to inmate use of computer equipment to the Warden, Superintendent of Education, Division Director of IT Security, and the Division Director of RIM.

2.4.4 Inmates working in specific prison industries and support services programs are allowed to use computers in conjunction with their assigned job duties, if these computers are not connected to any network outside the plant/work area. Supervisors are responsible for ensuring that inmate use of computer equipment is limited to the specific work program and for immediately reporting any violations relating to inmate use of computer equipment to the Warden, Division Director of Prison Industries or Division Director of Support Services as applicable, Division Director IT Security, and the Division Director of RIM.

2.4.5 Inmates who are not engaged in the programs referenced above are not allowed to use computers and related equipment without priorauthorization from the Division Director of RIM and the Division Director of IT Security. Wardens or Division Directors may submit a formal request through the online IT Requests System:

•Detailed objective of allowing the inmate(s) to use the computer equipment;

•Names and SCDC ID numbers of all inmates who will use the equipment;

•IT decal numbers of all equipment to be used by the inmate(s);

•Software that the inmate(s) will use;

•Employees responsible for supervising inmate(s) using computer equipment; and

•Detailed provisions made to ensure that the inmate(s) do not violate policy in his/her use of computer equipment.

•

2.4.6 Under no circumstances are inmates allowed to use computers with direct access to the Agency

network or to the Internet. Any network connection outside the educational lab/immediate work area must have written authorization by the Division Directors of RIM and IT Security, and shall have appropriate safeguards in place to limit inmate access to only that which is required and approved.

2.4.7 Inmate use of computer equipment is strictly limited to the assigned duty or to the educational/vocational objective. Inmate personal use of computer equipment is prohibited.

2.4.8 Inmate use of mainframe terminals and fax machines is prohibited.

2.4.9 Inmates are not allowed to use any computer, printer, scanner, or copy machine to reproduce legal documents (i.e., writs, extraditions, appeals, etc.) or any document that is not strictly related to the business use of the device.

2.4.10 Inmates are not allowed access to personal or confidential/restricted information concerning employees, inmates, or others.

2.4.11 Inmates are not allowed to remove computer equipment, removable media (diskettes, CDs, DVDs, USB drives), or printed materials from the classroom or other area in which he/she is authorized to use the computer equipment.

2.4.12 Inmates will not be given printed copies of any automated data except that relate to his/her own E. H. Cooper Trust Fund account, his/herapproved visiting list, or other data specifically authorized by applicable Agency policy.

2.4.13 Inmates will not be permitted access to any computer rooms unless accompanied and continually supervised byan authorized SCDC employee.

2.4.14 The Division of RIM Help Desk will maintain an inventory of all computer equipment being used by inmates, a list of inmates authorized to use computer equipment, and a list of employees responsible for supervising the inmates.

3. CONFIDENTIALITY OF DATA:

3.1 SCDC Deputy/Division Directors will determine how information pertaining to their areas of responsibility is classified as public or confidential, and will ensure that appropriate SCDC policies are regularly updated to include these classifications in accordance with SCDC Policy GA-06.05, "IT Security," Section 3.1.2, and applicable state and federal laws, and other regulations that may legally apply to SCDC's information.
3.2 If files, documents, records, etc., contain more than one type of data, it shall be classified and protected according to the highest level of data contained.

3.3 Each employee shall receive training in how to treat data of all classifications.

3.4 If an employee receives a request to disclose data that is not part of his/her regularly assigned job duties, he/she should refer the request to his/her supervisor. Freedom of Information Act requests should be forwarded to the Office of General Counsel.

3.5 Confidentiality Agreement: In order to ensure that all employees are aware of the importance of confidentiality as it pertains to the improper dissemination or sharing of information, all prospective employees must sign a Confidentiality Agreement (Appendix B/SCDC Form 13-53) during the pre-employment process. The Division Director of Human Resources or designee will be responsible for maintaining the signed Confidentiality Agreement in the personnel file of each active employee (including those hired prior to the effective date of this policy). (See SCDC Policy GA-06.05, "IT Security, Sections 1.3.3.2 and 6.1.4.1).

3.6 Reports containing restricted and/or confidential data will be subject to the following procedures:
3.6.1 Each Deputy Director, Division Director, and Warden will be responsible for designating an employee(s) in his/her area to be responsible for the following:
3.6.1.1 Maintaining a list of reports received containing restricted and/orconfidential data;

3.6.1.2 Ensuring the security and destruction of restricted and/or confidential reports; and
3.6.1.3Submitting a list of restricted and/or confidential data reports that are no longer needed (as determined by the Deputy Director, Division Director, or Warden) to the Division of RIM.

3.6.2 Reports containing restricted and/or confidential data are required to be under the control of authorized employees at all times. Printed reports containing confidential data must be stored in locked areas when not in use.

3.6.3 Printed reports containing restricted and/orconfidential data may be picked up from the Central Office Computer Room and signed for by the authorized employee. Any printed reports distributed by mail or other means will be enclosed in sealed packages addressed to authorized individuals only and will be clearly marked "CONFIDENTIAL" or "RESTRICTED."

3.6.4 Reports containing restricted and/orconfidential data authorized for use by a division, institution, or office will not be transferred or loaned to another division, institution, or office.

3.6.5 All printed reports containing restricted and/orconfidential data must be hand carried to the Central Office or Institutional Mail Room for appropriate shredding when no longer used. All shredders must be approved by the Division of IT Security as appropriate for the data classification of the material to be shredded.

3.7Procedures for the handling of electronic files containing confidential data:
3.7.1 Files containing restricted and/or confidential data will not be stored on local hard drives (i.e. C:). These files will be stored on network drives (i.e. H:, S:) which are physically located in a secure area managed by the Division of RIM, with encrypted backups stored off-site.

3.7.2 Files containing restricted and/or confidential data will not be stored on removable media such as diskette, CD/DVD, USB drives, etc. If a business need requires transmittal of confidential data to an outside party using removable media, users should contact the Division of RIM for assistance.

3.7.3 Files containing restricted and/or confidential data will not be stored on any type of internet "cloud" storage such as Google Drives, Skydrive, Dropbox, etc. If a business need requires transmittal of restricted and/or confidential data to an outside party via the Internet, users should contact the Division of RIM for assistance.

3.7.4 Files containing restricted and/or confidential data will not be sent to any person outside the Agency using unencrypted e-mail. If a business need requires transmittal of restricted and/or confidential data to an outside party via e-mail, users may encrypt these e-mail messages by inserting the [ENCRYPT] tag in the subject line of the e-mail. The tag may be inserted anywhere in the subject line, but must be typed exactly as shown including the brackets "[" before and "]" after the word ENCRYPT. Please contact the RIM Help Desk with any questions regarding the encryption of e-mail messages.

3.7.5 In order to prevent potential loss of restricted and/or confidential data in equipment disposal, the Division of RIM will institute procedures to completely erase or physically destroy hard drives in network attached storage, copiers, etc., prior to their disposal.

4. ACCESS REQUESTS:

4.1 The Division of RIM will assign a unique User ID to each person requiring access to any computer application, including e-mail, the Internet, and mainframe systems. Employees are required to change and secure his/her password, and are required to use the system as detailed in this policy in Section 2, "Acceptable Use."

4.1.1 The Division of RIM will create and maintain various types of user accounts (e.g., individual, group, system, application, guest/anonymous, administrator and temporary), using the account type with the least privileges required to meet the needs of the Agency. (See SCDC Policy GA-06.05, "IT Security, Section 2.1.2.1).

4.1.2 Any SCDC Manager that requires the use of guest/anonymous or temporary accounts must notify RIM as soon as the account is no longer required. RIM will then terminate or disable the account. (See SCDC Policy GA-06.05, "IT Security," Section 2.1.2.4).

4.2 The Division of RIM will assign major functions within each application system unique "security roles". For example, "view inmate transfer history", "transfer an inmate", and "modify inmate transfer history", are functions within the Inmate Transfer/Count system that are each assigned a unique "security role". Depending upon the application system, employees may also be limited to only access information concerning their institution or organizational unit. With this mechanism, employees can be granted access to individual functions within applications systems by being issued specific "security roles" by the Division of RIM. (See SCDC Policy GA-06.05, "IT Secuirty," Section 2.1)

4.3 SCDC Managers are responsible for ensuring that employees under their supervision have appropriate access to SCDC computer systems as required by their job duties, that they are trained to use the systems, and that they comply with Section 2, "Acceptable Use," of this policy. SCDC Managers are responsible for reporting personnel changes, changes in job duties, inappropriate computer access, and system security breaches as soon as possible to the Division of RIM so that computer access is revised as appropriate.

4.4 To request access to an application system on behalf of theiremployees, Managers will specify each data entry/access "function" needed by the employee using the automated Access Requests System. Managers will also submit requests to remove data entry/access using the Access Requests System. (See SCDC Policy GA-06.05, "IT Security," Section 2.1.2).

4.5 If the Manager's instructions are clear, access will be granted to the requested application functions that are consistent with the employee's job and position responsibilities. In cases where a requested function is not typically granted to employees in this position, the Help Desk will forward a copy of the request to the application owner for disposition. Access to these functions will be granted only if the application owner approves the request. (See SCDC Policy GA-06.05, "IT Security," Section 2.1.2).

4.6 The Help Desk will send new users written instructions for signing on the system, including their User ID and a temporary password. The first time a user logs in, the system will force him/her to create and verify a new password. Passwords must be eight characters in length and include at least 1 character, 1 number, and 1 special symbol (# $ @). The password must be a combination of letters and numbers and special symbols that the user has not used previously. Passwords should not be common words, or based on personal information such as usernames, social security number, etc. (see SCDC Policy GA-06.05, "IT Security, Section 2.6.1.4 for more guidance).

4.7 SCDC Managers must request access via the Access Requests System for all new employees under their supervision, even in cases where the employee is transferring from another SCDC position. To avoid a lapse of system access, SCDC Managers should do so immediately when an employee transfers into their supervision. (4-4101) (See SCDC Policy GA-06.05, "IT Security," Section 2.1.2).

4.8 Privileged User Accounts shall be assigned, controlled and monitored by the Division of RIM through their internal procedures. If an employee requires a privileged user account, his/her supervisor must request access via the Access Requests System as described above. Privileged user accounts must be approved by the Division Directors of RIM and IT Security (See SCDC Policy GA-06.05, "IT Security," Section 2.1.2.10).

4.9 SCDC Managers must request access for contractors, vendors, and other third parties that require an SCDC user account using the Access Requests System.

5. ACCESS TERMINATIONS:

5.1 The Division of RIM will automatically remove system access for employees who leave the Agency and when an employee changes positions. Because this action is dependent upon entries into the personnel management system, removal of system access may not be immediate. (See SCDC Policy GA-06.05, "IT Security," Section 2.1.2.5).

5.2 Whenever an employee,contractor, or other third party terminates unexpectedly, or there is a need to immediately revoke a user's access to the automated system for other reasons, the manager will notify the RIM Help Desk or the Division Director of RIM. The Division Director of RIM will authorize appropriate personnel to either delete the user ID (termination) or make the appropriate access limitations as required.

5.3 Annually and upon request, the Help Desk will provide each application owner with a list of employees who have access to the systems for which they are responsible. The application owner will review the system access listing and report inconsistencies or issues to the Help Desk. (See SCDC Policy GA-06.05, "IT Security," Section 2.1.2.13).

5.4 RIM shall suspend mainframe user accounts after 45 days of inactivity (See SCDC Policy GA-06.05, "IT Security," Section 2.6.1.5).

6. REPORTING PROBLEMS/REQUESTING TECHNICAL SUPPORT:

6.1 The RIM Help Desk is the primary point of contact between SCDC employees and the Division of RIM. The Help Desk will:

•Track all reports of equipment malfunctions and system problems, and inform affected users of the status of problems and of scheduled down time;

•Re-instate revoked User IDs;

•Coordinate requests for system access with appropriate "application owner" and grant employee access accordingly;

•Maintain an inventory of all IT assets, including computer terminals, personal computers, printers, fax machines, pagers, cell phones, phone lines, software licenses, warranties, service contracts, network hardware, and wiring configurations;

•Designate a "RIM user liaison" for each division and each institution; the "user liaison" will assist the Help Desk in tracking equipment and assisting other users at their site.

6.2 Employees will notify the Help Desk of equipment malfunctions and system problems, providing details of the problem and the decal number of affected equipment. When experiencing hardware problems, employees are encouraged to consult their institutional/divisional liaison for assistance before placing a call to the Help Desk.

6.3 Help Desk staff determine the scope of reported problems and will enter all reports into a tracking system. If unable to solve the problem at the time it is reported, they will "escalate" the problem to the appropriate branch chief or to a service provider as appropriate. In the event an entire institution or a significant number of employees are effected, the Help Desk will notify the Division Director of RIM and other SCDC management as appropriate.

6.4 RIM branch chiefs are responsible for informing the Help Desk of the disposition of reported problems. When informed that a problem is resolved, the Help Desk will notify the original caller and SCDC management as appropriate and will "close" the problem in the tracking system.

6.5 RIM staff and contracted service technicians will remove/affix decals to equipment being replaced, will document all equipment changes using form, and will provide a copy of SCDC Form 13-54, "IT Asset Change" (see Appendix C) to the institutional liaison and the Help Desk. Institutional liaisons are responsible for ensuring that service technicians adhere to those procedures and will inform the Help Desk of inconsistencies/problems. Upon receiving a copy of the "IT Asset Change" form, the Help Desk will enter all changes into the IT asset tracking system.

6.6 The problem tracking system will serve as a knowledge base to facilitate prompt resolution of problems. The Help Desk manager will submit a monthly report to the Division Director of RIM that documents all serious system outages for the month, including telephone outages and widespread system down time.

7. TRAINING:

7.1 The Division of RIM will provide regular training sessions on basic use of SCDC mainframe systems, e-mails, and other computer applications.

7.2 The Division of RIM will work with application owners to develop detailed training materials and training sessions for specific application systems. Application owners and SCDC managers will advise the Division Director of RIM of specific training needs and/or shortcomings in existing training curriculum.

7.3 SCDC Managers are responsible for ensuring that employees under their supervision are properly trained to use IT resources and that they properly use IT in accordance with SCDC policy. (4-4101)

8. DATA LOSS RESPONSE PLAN:

8.1 SCDC Managers must notify the Division of RIM and the Division of IT Security immediately if they suspect a breach of security in any SCDC computerized system. The Division of RIM and the Division of IT Security will investigate the report and determine, as soon as possible, the extent of any potential unauthorized data access.

8.2 In the event that a security breach of an SCDC computerized system containing personal identifying information has been substantiated, the Division Director of RIM and/or the Division Director of IT Security will notify the Agency Director, Deputy Director for Administration, Inspector General, General Counsel, and other executive staff as appropriate.

8.3 The Agency will provide notice to all affected persons as required by Section 1-11-490 of the Code of Laws of South Carolina, by the safest andmost expedient means possible.

9. DEFINITIONS:
Information Technology Resources - Information technology (IT) resources encompass all technology used to collect, manage, exchange, and display information, and all devices that transmit electrical or optical signals for the purpose of providing information, as well as all data, information, reports, and documents derived from automated systems. Examples of IT resources include:

•Personal computers and component parts (monitor, keyboard, mouse, etc.);

•Mainframe terminals (CRTs);

•Printers, copiers, scanners, and fax machines;

•Diskettes, CD ROMs, DVDs, backup tapes, and USB drives;

•ID card readers, bar code scanners, and PCI compliant card readers;

•Fingerprint scanners;

•Computer operating systems and application software (word processing, spreadsheets, database management software, and software developed or procured to provide a specific function);

•Network cards, modems, routers, hubs, and controllers;

•Telephones, cell phones, tablets, Personal Digital Assistants (PDA), pagers, and accessories;

•Un-interruptible power supplies (UPS);

•Computer and telephone wiring and connectors;

•Cameras and videoconferencing equipment (excluding analog video surveillance cameras);

•Computer printouts (e.g., computer generated lists, rosters, charts, graphs, and presentations);

•Word processing documents, spreadsheets, and database files;

•Electronic mail and calendars, and mainframe messages;

•Audio/Visual Equipment (Projectors, TV's, DVRs, and DVD/VCR/CD Player/Recorders);

•Professional Printing Equipment and Software Services;

•Outside sources of Information Technology Services (Document Scanning, Programming Services, Hardware/Software Services).

Computer Application - A general term describing computer software that performs specific functions. Computer applications include commercial software such as Microsoft Word, Excel, PowerPoint, etc., as well as software developed by SCDC staff. Examples of computer applications that operate in the mainframe include the transfer/count (TRANCT) and the earned work credit (EWC) applications.

Application Owner - An SCDC manager or employee designated by RIM who is responsible for authorizing changes to the application system and approving access to the system.

RIM Institutional Liaison -The Division of RIM will designate a person at each institution, referred to as the RIM institutional liaison, who will serve as a point of contact between RIM and the institution.

RIM Divisional Liaison - The Division of RIM will designate a person from each division, referred to as the RIM divisional liaison, who will serve as a point of contact between RIM and the division.

E-mail- Refers to electronic mail, and provides the ability to send and receive messages to other computer system users, both within SCDC and external to SCDC using the public Internet. When referred to in this policy, e-mail includes the mainframe-based messaging facility.

User- A person authorized to use a computer system. Users of SCDC applications and IT resources include SCDC employees, persons employed by other State agencies, contractors, and in some limited cases, inmates.

User ID- An account, identified by a string of up to eight letters and numbers, established for an individual that enables a person to access a computer system. Employees have a User ID to access the mainframe and a User ID to access server based systems (in general, the two User IDs have matching names).

Password -To access mainframe or server based systems, users must enter their User ID and a password. Passwords must be eight characters in length and include at least 1 character, 1 number, and 1 special symbol (# $ @). The password must be a combination of letters and numbers and special symbols that the user has not used previously. Users must not share his/her password with anyone.

Web Based Application - A system developed or purchased by SCDC that operates using web browser software.

SCDC Intranet - Web based applications that can only be used by SCDC users and are not available across the public Internet.

Public Web Page - Web based applications that are accessible to the public across the Internet.

Modem- In SCDC policy, "modem" refers to a device that connects computer equipment to any network outside of SCDC's local area network, either through the public phone system or through cellular communications.

Terminal - A device used to access mainframe applications. At SCDC, the term "CRT" is sometimes used to describe a mainframe access terminal.

PC - Personal computer.

SCDC Managers or Managers - Associate Wardens, Assistant Division Directors, Wardens, Division Directors, Regional Directors, Deputy Directors, and the Agency Director.

s/Bryan P. Stirling, Director

Date of Signature

ORIGINAL SIGNED COPY MAINTAINED IN THE OFFICE OF POLICY DEVELOPMENT.

APPENDIX A

## The Law in the United States

Software is automatically protected by federal copyright law from the moment of its creation. The rights granted to the owner of a copyright are clearly stated in the Copyright Act, Title 17 of the U.S. Code. The Act gives the owner of the copyright "the exclusive rights to reproduce the copyrighted work" and "to distribute copies...of the copyrighted work" (Section 106). It also states that "anyone who violates any of the exclusive rights of the copyright owner...is an infringer of the copyright" (Section 501), and sets forth several penalties for such conduct.

Those who purchase a license for a copy of software do not have the right to make additional copies without the permission of the copyright owner, except (i) copy the software onto a single computer and (ii) make "another copy for archival purposes only," which are specifically provided in the Copyright Act (Section 117). The license accompanying the product may allow additional copies to be made. (Users must be sure to review the license carefully.)

Software creates unique problems for copyright owners because it is so easy to duplicate, and the copy is usually as good as the original. This fact, however, does not make it legal to violate the rights of the copyright owner. Although software is a new medium of intellectual property, its protection is grounded in the long-established copyright rules that govern other more familiar media, such as records, books, and films.

The unauthorized duplication of software constitutes copyright infringement regardless of whether it is done for sale, for free distribution, or for the copiers own use. Moreover, copiers are liable for the resulting copyright infringement whether or not they knew that their conduct violated federal law. Penalties include liability for damages suffered by the copyright owner plus any profits of the infringer that are attributable to the copying, or statutory damages of up to $100,000 for each work infringed.

The unauthorized duplication of software is also a federal crime if done "willfully and for purposes of commercial advantage or private financial gain (Title 18 Section 2319(b))." Criminal penalties include fines of as much as $250,000 and jail terms of up to five (5) years.

APPENDIX B

SOUTH CAROLINA DEPARTMENT OF CORRECTIONS
Division of Human Resources
Confidentiality Agreement

Purpose: To maintain the confidentiality of any and all Agency records, including those accessible through the South Carolina Enterprise Information System (SCEIS) and SCDC automated systems.

The South Carolina Department of Corrections maintains personal and confidential information regarding many citizens: registered victims and witnesses; visitors and volunteers; current and former inmates; and current and former employees.

As an employee with the South Carolina Department of Corrections:

I understand and agree that I must keep this information confidential and must not disclose this information to persons within the Agency who have no job-related need to know the information or to persons outside the Agency without proper authorization from the Agency.

I agree that I will not, at any time during or after my employment with the Agency, directly or indirectly, orally or in any written form, disclose any of this confidential information unless such disclosure is required as a part of my job, pursuant to an appropriate audit, or by proper authorization from the Agency.

I also agree that I will not remove any of this confidential information from the Agency without prior, proper authorization from the Agency.

I also agree that if I receive a subpoena, Freedom of Information Act request, or other request for disclosure of any of this confidential information, I will forward that request to the appropriate person designated by the Agency to respond to the request.

I am aware that SCDC Policies ADM-15.05, "Security And Use Of Information Technology," ADM-15.03, "Information Technology Requests," and ADM-15.14, "E-Mail Retention, Backup, And Archival," contains specific information concerning SCDC requirements for Information Technology and Security.

And, I understand that if I breach this Confidentiality Agreement, I am subject to correctiveaction by the Agency, up to and including termination.

| | |
|---|---|
| EMPLOYEE ID | EMPLOYEE NAME (Please Print) |
| DATE | EMPLOYEE SIGNATURE |
| DATE | SIGNATURE OF AGENCY WITNESS |

SCDC FORM 13-53 (Created September, 2013) FOR USE BY HUMAN RESOURCES (HR) STAFF ONLY